Web Sites

Georgia Tech Wearable Motherboard

www.gtwm.gatech.edu

You've read MAJ Phillip G. Burns' article on the Combat Wireless Health Monitoring System, now learn more about the Georgia Tech Wearable Motherboard (GTWM)—the "smart shirt" prototype that started it all. Learn more about the garment that uses optical fibers to detect bullet wounds and special sensors that interconnect to monitor the body's vital signs during combat conditions. Also learn more about why the GTWM is needed in combat; next-generation GTWMs; the project team and the impact of their research; and national media coverage on the technology.

Information Assurance Support Environment – Public Key Infrastructure (PKI)

http://iase.disa.mil/pki

After reading Susan Chandler and Jerrod Loyless' article on the DoD's PKI—a service of products which provide and manage X.509 certificates for public key cryptography—you may want to visit the DoD's "one-stop shop" for information assurance and PKI knowledge and training. You can receive guidance on policy issues; get information on the DoD PKI's around-the-clock Help Desk; connect with the PKI Certificate Policy Management Working Group; download training guides, memos, and other PKI documents; receive DoD PKI online training; read government memoranda and training guides regarding PKI; link to other Web sites of interest; and learn about the External Certification Authority Program. There is also information on the DoD's expansion of their Secret Internet Protocol Router Network (SIPRNet), and how SIPRNet smart cards will increase security levels.

Remarks by the President on Securing Our Nation's Cyber Infrastructure

www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

Summer Olmstead and Dr. Ambareen Siraj—in *Cyberterrorism: The Threat of Virtual Warfare*—delve into an issue that President Barack Obama addressed in his May 29, 2009 speech covering the great promise but great peril of cyberspace. President Obama's speech covers cybercrime in its many forms: identity theft, privacy violations, the economic risks to e-commerce, ATM robberies, and stolen intellectual property. He also addresses national security issues and the recent cyber intrusion into our power grid. The President's main focus, though, is our military networks, which have faced the most serious cyber incidents and infections via malware. After discussing these issues, the President outlines a new approach and a range of actions in five key areas.

Information Assurance Support Environment – DITSCAP Transition to DIACAP

http://iase.disa.mil/diacap

In this issue's *Certification and Accreditation of SOA Implementations: Programmatic Rules for the DoD*, the authors discuss the DoD Information Assurance Certification and Accreditation Process (DIACAP), a process to ensure that risk management is applied on Information Systems from an enterprise view. This Web site gives an overview of DIACAP; provides guidelines in the transitioning from the DoD's Information Technology Security Certification and Accreditation Process (DITSCAP); offers access to the signed DIACAP in its entirety as well as to National Information Assurance Certification and Accreditation Process Instruction; and links users to online DIACAP training.

Interview: John G. Grimes

http://defensesystems.com/Articles/2008/11/Interview-with-John-Grimes.aspx

Assistant Secretary of Defense for Networks and Information Integration/DoD CIO (and frequent CrossTalk contributor), the Honorable John G. Grimes, believes that organizations have to work together for interoperability. In this interview from *Defense Systems* magazine, Grimes discusses issues including the alignment of the military services' IT infrastructures, the challenge of information sharing among government agencies, and the threat of cyberattacks. He also discusses the DoD's movement to service-oriented architecture, which is providing great opportunities for the DoD to quickly deploy Web services that make information available across organizational boundaries.

The Lean Systems Engineering (LSE) Working Group

http://cse.lmu.edu/about/graduateeducation/systemsengineering/INCOSE.htm

The goal of the LSE Working Group is to strengthen the practice of SE by exploring and capturing the synergy between traditional SE and Lean. Through the Web site, the group: applies the wisdom of Lean thinking into SE practices, people, processes, and tools for the most effective delivery of value to program stakeholders; formulates the body of knowledge of LSE; and develops and disseminates training materials and publications on Lean SE within the International Council on Systems Engineering community, as well as with industry and academia. Learn more about the group—its members, history, publications, accomplishments, and mission—as well as receive access to several resources detailing what Lean SE is all about.

Software Engineering Process Group (EPG) Guide

www.sei.cmu.edu/reports/90tr024.pdf

Read the guide that revolutionized software EPGs and told readers that "it takes tremendous energy to counter our own and others' resistance." Even after 19 years, Priscilla Fowler and Stan Rifkin's work is still a must-read for anyone wanting to establish a software EPG. Emphasizing the "what" over the "how," the guide offers a basic introduction to the subject and provides guidance for initiating and sustaining an improvement program in an organization. The guide is as much concerned with the human side of stimulating a higher quality process as with the technology of improved processes.